FTC FinTech Forum: Artificial Intelligence and Blockchain
March 9, 2017
Panel 2
Transcript

COLIN HECTOR: Great. My name is Colin Hector. I'm a staff attorney in the Federal Trade Commission's Division of Financial Practices. And to my left is Elizabeth Kwok, who's an investigator in the FTC's Division of Financial Practices.

As with our AI panel, we are very fortunate to have a wonderful bunch of panelists whose accolades and experience is simply too numerous and extensive for me to give fair treatment of. So I'm going to give a one or two-sentence introduction for each of the panelists to our left. And then we can dive into discussing some of the issues that Peter previewed for us.

Perianne Boring is the founder and president of the Chamber of Digital Commerce, the world's largest trade association representing the block chain industry. Under her leadership, the chamber leads several key industry initiatives, including the Blockchain Alliance, the Global Blockchain Forum, and the Smart Contracts Alliance.

Kyle Burgess is been gracious enough to come here on sort of very late notice. She's the director of strategy and editor-in-chief at Consumers' Research. Unfortunately, two of our panelists today weren't able to make it-- Joe Colangelo and Zooko Wilcox.

Justin Slaughter serves as chief policy adviser and special counsel to commodity futures trading commissioner Sharon White Bowen, and has advised the Commissioner on all matters of policy, politics, press, and law regarding the future and swaps market.

Christina Tetreault is a staff attorney on Consumers Union's financial services program team, specializing in banking, payments, and financial technology. Christina represents the consumer interest organization segment on the steering committee for the Federal Reserve's Faster Payments Task Force.

Peter Van Valkenburgh, who you just heard from, is the director of research at Coin Center, the leading nonprofit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as bitcoin.

And Aaron Wright is a clinical professor at Cardoza Law School and director of the school's Blockchain Project, an initiative examining the legal and policy implications generated by blockchain technology. He has a forthcoming book about blockchain technology and the law, under contract with Harvard University Press.

I'm gonna turn it over to Elizabeth to begin our discussion.

ELIZABETH KWOK: Great. Thank you so much, Colin. So as Peter's presentation pointed out, this is a very broad topic. And so before we move into more specific areas, I wanted to give our panelists an opportunity to provide any additional distinctions or helpful background before we go on. So if anybody has anything to say. Otherwise, I have specific folks I can start with.

AARON WRIGHT: So I thought Peter's presentation was great. The one thing that I may just add to it is I think that because that sack of technology which was described watching technology more broadly it exhibits in core characteristics, which I think are important in understanding the technology. I mean, one, because of the peer-to-peer network, it's disintermediate and transnational. It's a lot like email in that sense.

So these networks are supported by computers around the globe. The bitcoin blockchain supported by at least 5,000 full computers that store copies of the blockchain. Because it's disintermediated and transnational, it actually becomes highly resilient.

So because the data is replicated in such a massive way, it's really hard to remove data once it's stored. And because it relies on that, that consensus mechanism, the database-- it isn't fully mutable. I think that's really a design choice. But at least at a minimum, it's tamper-resistant.

And I think the last thing-- there's a couple other characteristics. But the last one that may be useful for the purpose of this conversation is that other data that can get stored is also not just flat file data, but also programs. Those programs are generally called smart contracts.

So when you combine that disintermediated and transnational nature of a blockchain with the ability to actually run programs on some of these blockchain-based systems, you can actually deploy arguably for the first time, truly autonomous software-- autonomous in the sense that no one party controls its execution and validation. So I think that's important.

Great. Great. Thank you so much, Aaron. And Peter, you had touched upon two things that I wanted to you go perhaps just a little bit more into detail from your presentation. The first is this concept of blockchain versus distributed ledger technology at large, such as Corda. And I wonder if you could provide just maybe a few more distinctive points for our audience.

PETER VAN VALKENBURGH: Sure. So I mean, a lot of it is just terminology, I think. I do think that primarily bitcoin was this headline-making innovation for being this completely decentralized, completely denationalized money. And it showcased some technologies that had existed for a long time-- cryptographic hash functions, and even using cryptographic hash functions to create incentives for our participants. So hashcash is a great example.

And oh, shoot. What's the email spam protection prevention?

AARON WRIGHT: That was hashcash.

PETER VAN VALKENBURGH: That was hashcash. So just in order to send an email, you'll have to find a collision in SHA-256.

AARON WRIGHT: Yeah. SHA-256.

PETER VAN VALKENBURGH: And that adds a small minor cost to sending an email, which makes it cost-prohibitive to sending spam, because for a normal individual, oh, my computer you know, it got a little hot, ran a little hot for a little while. It sent an email. I don't care.

For someone trying to send millions of e-mails, their computer's really going to heat up, need a lot of electricity. These were technologies that existed. They got recombined in bitcoin in order to do something novel and something exciting.

And I think what that did was send a signal to especially-- so, legacy financial institutions, for example. It's like, oh, well, we can do digital bearer instruments and move money across the world at amazing speeds and low fees. And this compared to the correspondent banking system, or even the commercial paper world, or anything that we know today, is rather amazing. Let's take these innovations and do something with them.

And then the branding aspect is, I think, a big part of it. Is it blockchain technology at that point? We're not going to use bitcoin because it's too big. It's too open. Maybe we can call it something else. Then blockchain, lets call it DLT, that sounds very official.

And as Aaron was saying, I actually don't like DLT personally for thinking about these technologies, because it's not always a ledger. The ledger is one human understood data structure. Another data structure is the sort that a computer would use to run programmatic logic, and actually just store variables and have state, state that's more complicated than just credits and debits.

So DLT is a thing. But I think it's a minor subset. It's where you're really just going to build a network explicitly for the purpose of sharing this ledger of credits and debits or some sort of financial transaction.

PERIANNE BORING: That is one of the biggest questions that the industry and the community is discussing. What is the difference between blockchain and DLT. There's kind of a lot of buzzwords we're throwing around.

David Rutter, who is the founder of R3, which has been mentioned, which is the consortia of banks. They have over 50 members of banks that are working together to build distributed ledger technology solutions for banks. And David will be speaking at Georgetown University next week on this exact topic.

And there was a little bit of a scandal. But it was really more misinformation in the media recently that there was some presentation where R3 said, we don't need blockchain. Well one, that's not entirely correct. But what it comes back to is regulated financial institutions have a lot of regulatory constraints. And we'll talk more about those throughout the panel.

The biggest one being in an open network, like bitcoin, which Peter's done a good job of explaining. Anyone can participate in the bitcoin network, which is one of the most beautiful things about this technology. But for regulated financial institutions, there's a lot of questions around what is appropriate. The biggest one being sanctions.

So if a bitcoin was mined in North Korea, and somehow that bitcoin ends up in one of the US banks, is that an OFAC violation? Well, we don't actually know, because we don't have

clarity from the regulators on those types of question. So while the industry is incredibly nascent, not all those questions have been figured out quite yet.

A lot of the banks are building their own private networks. and that's a lot of what DLT is about and what it's for. And there is an important place for it. And it mostly fits in in regulated industries. Banking obviously. But also insurance. There's an insurance consortium called B3i, the largest insurers and re-insurers in the world are participating in that, and in healthcare.

JUSTIN SLAUGHTER: I'd also make one additional point. When you're talking about these highly regulated institutions, you're completely right. Right now the regulators have been pretty close to silent. Cause my agency is one of the only ones to do anything on this, which is only be an enforcement action of bitcoin, let alone a blockchain.

That said, there's a real significant divide here in terms of how regulators think about this right. For transactions that involve one entity with another external entity, the regulations are inherently greater, right? And for ones involving internal record-keeping, there are still regulations there. But oftentimes there's less. There's certainly at least different consumer protection issues.

So to some extent, I think we're going to have to figure out to what extent there need to be regulations on inter-entity transactions, versus ones that are focused on internal entities.

PERIANNE BORING: We've spent quite a bit of time with the CFTC. And I completely agree. You guys have done an amazing job.

JUSTIN SLAUGHTER: Thank you for that. I don't think I deserve that. But thank you.

PERIANNE BORING: The CFTC has some limitations, though, in that your jurisdiction is very narrow.

JUSTIN SLAUGHTER: That's true. This is an area where the regulators don't yet know who has responsibility for this, which hopefully will lead to positive synergies between us and the FTC, maybe the FCC, maybe other entities. And you know, I've been in politics and government long enough to know that usually assume that where there's a dispute over jurisdiction, things will get worse rather than better. But hope springs eternal. Especially on [INAUDIBLE], because of the desire for effective, smart regulation, rather than just people throwing up fences.

ELIZABETH KWOK: Great. And both of you have actually touched upon this, but for our consumers out there, blockchain is obviously a buzzword. Cryptocurrency is a buzzword. But today, we'd really like to focus on kind of all of these growth areas.

And so we can start with Perianne. But what do you see growth in this industry at large looking at? Where are the different places that consumers can really be paying attention for other use cases aside from cryptocurrencies, perhaps?

PERIANNE BORING: We're seeing a lot of action in the healthcare space. In fact, next week, I mentioned there's an event in Georgetown that we're hosting. And in conjunction with that, the Department of Health and Human Services in ONC are hosting the first ever blockchain code-a-thon. That will be sponsored by a government agency. And the Chamber of Digital Commerce is co-hosting this with HHS and ONC.

There's been quite a bit of activity and dialogue in terms of how blockchain could be used in the health care industry. And we're still debating that. And this is something that we built upon all the way back from September of last year.

HHS had what they called the Blockchain Challenge. And it was essentially a call for research, a call for papers. It happened to be one of the most successful call for papers HHS had had in decades. They received over 70 submissions from technology companies that really had not engaged with HHS previously. So they were very encouraged by the amount of peepers that they received.

And so the next step they said, well, I think there's something here. Everyone is showing up. Everyone is submitting papers. They had hundreds of use cases that were presented.

So then HHS said, you know what? We need to spend more time on this. The next step is we need to put the technology in our hands. So what we pitched to them was let's do a code-a-thon. And so that's what we're going to do.

Well a hack-a-thon, code-a-thon. The government didn't like the word "hack" as much. But we're calling it a code-a-thon. But you guys get the point.

And HHS and ONC hasn't really quite determined if blockchain will be a useful technology for health care. But we're going through that. And it's really important as we have these discussions that we also establish that we're in a very nascent industry. It's incredibly early days.

So a lot of times people have these huge expectations. Look at the growth of the internet. It took decades to build all those layers from email and the other protocols.

So just know that it is early days we're looking at. We don't have all of the solutions. But what's most important is that we have the opportunity to text. And that we have an open dialogue with the regulatory community.

AARON WRIGHT: I would have like the internet, certain ideas. You know, early on with the internet, people realized back in the '90s that you could stream video. But it took until mid-2000's before YouTube really took that mantle and built a robust service. So you know, the applications for blockchain technologies are broad.

I mean, Peter touched on some of them. So one is just payment systems. Right? That's bitcoin. Bitcoin is fundamentally a payment system, or at least initially it was conceived as a payment system.

The second one is, since you can run these autonomous programs, the notion has emerged that you can begin to model out certain legal agreements or all or parts of legal agreements using this code. So since you can transfer value with a blockchain-based network, usually in the form of a digital currency, you can begin to then add additional logic on top of that-- if and then statements-- and take in outside data feeds in order to actually make these dynamic agreements that operate fairly autonomously.

So that could be all or a portion of an agreement. So when you begin to think about that-- and I think especially in the financial services industry, they began to think about that. And they said, hey, I can transfer value. And I can do some higher level logic. Well, then I can begin to model out certain complex and standard financial transactions.

So because a blockchain can sort any data, it can also store things like represented versions of a security. So we can begin to not just transfer virtual currency, but we can begin to atomically swap a security. Right?

So right now it takes quite some time to transfer security to the various intermediaries that are involved. We can begin to actually do that in a much faster way. But beyond that, since we can actually model at this high level logic, we can do things like model out derivatives. We can build marketplaces that don't have an intermediary like NASDAQ or the New York Stock Exchange.

We can build decentralized marketplaces that can exchange those tokens, securities, that can actually be involved in the transfer of certain derivatives. So we're seeing that emerge in prediction markets.

Beyond that, because you can store data and it's really tamper-resistant, you can begin to actually just store flat information. That information can be used to correlate with other peer-to-peer networks. So we're seeing the emergence of actually like decentralized Napsters. Napster relied on a centralized index. A blockchain can serve as that index. So that could have some impacts on how we distribute media online.

Because blockchains are so tamper-resistant and resilient, another thought emerged. Hey, we have a lot of really important paper records. But if we look into the future 50, 100 years, I think it's plausible to assume we may not have paper records at that point in time. Maybe blockchains can be used to store really, really important paper records, things like voting records, which Peter mentioned; a title to land; things like a title to intellectual property; and other really important information can get stored on a blockchain in a machine-readable way so that other people can access that.

And the last area-- well, there's two more areas. Another area is with regard to organizations. So since you can transfer value, and you can model out these higher level logic using smart contracts, you can begin to conceive of building virtual corporations. And we've seen early indications of this. So instead of having corporations or other organizations governed by agreements, we can have organizations increasingly governed by code.

And the last category is really machine-to-machine interactions. So as we learned from the last panel, algorithms and algorithms embedded in machines are getting more and more advanced. At some point, those machines are going to transact with us. They're going to transact with one another.

And if they're going to do that, they're probably not going to rely on natural language agreements. So companies like IBM are going through the process of actually building out machine-to-machine transactions using a blockchain and smart contract base systems. And then that raises a number of additional questions about how can you actually use these smart contract based system to actually manage organizations.

This is the most futuristic aspect, but I think it's worth noting. But conceivably you could use these systems and algorithm-based systems running on blockchain to manage organizations themselves. That's called decentralized autonomous organization, or DAU. So that's kind of the universe of what we're talking about here.

And that interplays with a number of different areas of law. And obviously a lot of this has embedded in it financial aspects, because there is this value transfer characteristic of most blockchain-based systems.

PETER VAN VALKENBURGH: I think also mentioning as you did that this is a lot like what the internet looked like back when people were thinking, oh, we could put streaming video on this. It took time. It took higher level protocols. It also took scalability. It took computing power to ramp up, network throughput to increase.

And we are seeing that with blockchain technologies as well. So for anything that involves programmatic logic that is running on the blockchain data structure, on a massively replicated virtual machine, if you will, a global computer, this is what Ethereum seeks to build, for example and is building.

It doesn't benefit from parallelization like you might think. So yeah, the computers on the network are all running the computation that does something that allows an organization to come together of distributed participants, or does vote counting, or does any number of other things. The computation is running redundantly on every computer. And no computer can get ahead of any other, because this is a consensus algorithm.

So actually it doesn't scale globally the way you might think of a massively parallel computing system. It scales at the rate of the slowest machine on the system, in a certain sense. But that is not a death knell to this as an amazing technology, any more than the poor throughput of the internet in the 1990s was a death knell to Netflix. It's exciting, actually.

AARON WRIGHT: And this smart contract basis, they basically run code that you would expect in like the 1990s on a smartphone. But you know, like every technology, people working to improve those scalability issues. So it's conceivable. It's a plausible, that over time we'll see actually a faster, faster ability to run these types of software programs.

COLIN HECTOR: One followup on that-- I mean, we've already identified a lot of potential sectors where the benefits of blockchain will flow to. The question I have is, how does this look from the perspective of a consumer? In other words, are the benefits going to be transparent to them? Are there going to be sort of consumer products that are reflected in these changes? Or is it going to be something that more sort of operates in the background?

KYLE BURGESS: I think Perianne pointed out a very important thing, which is that we're in early days. And so three years ago when I met Perianne, actually, at a conference, you would hear a lot about financial inclusion. And it is really important. There are 2 billion people worldwide that are not banked. There are 9 million in America, I think 24 million in America that are underbanked. And you're going to hear a lot about the problems that blockchain can solve for those consumers.

But I think it's really important that consumer protection and consumer education comes first before consumers are really actively using this technology.

One anecdote. We host a conference every summer in Bretton Woods-- well, for the last two summers. We're doing it again this summer.

And I was explaining to one of the women who worked at the hotel where we host the conference what we were doing. She was very interested in the topic. And I was telling her what bitcoin is, what blockchain technology can do.

And I was like, but you know, you need to be careful. There are a lot of instances where people just lose a lot of money. And I explained a lot of the scandal that you may have heard about. And I really told her it's not a speculative-- well, it is used as a speculative tool. But that's not what you should use it for.

And even after giving her all of these warnings, she says, I'm going to go home and talk to my husband about how I can use this technology to make money. And I was just like, no. I think you heard nothing that I said.

So apart from just peer-to-peer transactions, you will hear a lot about financial inclusion efforts. One case-- I think it's called the Women's Annex Forum-- it's in Afghanistan. And they work with young women to help them have financial autonomy. They have kind of like an Amazon online system that they can use bitcoin to buy things where they can't actually participate in the marketplace locally because they can't go out unattended.

And so they might blog or something for bitcoin. And then they can use that bitcoin to buy something online. So there are examples of ways that bitcoin and other digital currencies are being used to improve financial inclusion. But I still think we're a little too early to say that this is the solution.

And going off a little bit of what Perianne said earlier, and also what Aaron said-- just lost my train of thought. Yeah. I'll stop there.

PERIANNE BORING: Well, certainly on financial inclusion, there's a very strong argument, again, because anyone can have access to this network. Think of the 74% of the world's population that does not have access to basic financial services. But a lot of people have these. In fact, we love these. We bring them everywhere. I brought mine on stage with me.

If you have access to a smartphone-- and in a lot of developing economies, especially all throughout Africa-- we have been able to bring mobile devices into financial services. But bitcoin and blockchain and cryptotokens and cryptocurrencies, the consumer, especially American consumers, we're really used to certain expectations, like being FDIC insured.

That just doesn't exist in the bitcoin economy. We don't have a lot of those same expectations. And everything you know about money and payments, you kind of have to just put that aside. This is a paradigm shift in terms of financial services and banking.

So as Kyle mentioned, education has to come first. The consumer has to understand what public and private keys. They have to understand how the technology works at a fundamental level.

And we're at a little bit of a disadvantage, because very few schools that have any coursework on this. There's very few places to get educated on these topics. I mean, our organization, Consumer's Research has done an amazing job. Coincenter has done an amazing job publishing a lot of publications to help educate the consumer.

But in order for this to benefit populations, we have to get over an educational hurdle first. And that's going to take time. Think about when we first started using computers. You don't just buy a computer and you just know how to use it overnight. It takes time.

You take computer classes. You take typing classes. Driving a car. You don't just wake up one day and start driving your car. First you ride in a car for many, many years.

You get a license by the government to use it. Not that I'm advocating that. There's rules to the road. But there is an educational element that has to happen.

COLIN HECTOR: Looks like both Christina and Justin want to add something. How about Christina first, then Justin. Then we'll come back to you, Peter.

CHRISTINA TETREAULT: Sure. I mean, coming back to this question. What are the consumer-facing applications that we're seeing right now? It's financial services has been said here. And that raises a number of concerns that Peter's presentation really referenced very well, which is you've got-- if you're using it as currency, or you're using it for these value transfers, you've got questions around the irreversibility. You've got the volatility question. You've got the gap in the legal protections.

So that's sort of one way that it's working right now. And that's problematic for a number of reasons. But the concern here, as was said, is there's a lot of work that needs to be done to lay the groundwork for people to really be able to use it as money, if that's what they choose to do.

To the question about how it's being used in the back of the house and what those implications are is that you've got companies, some of which names showed up in Peter's presentations, that are using it for back-of-the-house transactions. And that really has a different implication for consumers. It's not about understanding what the risks are or anticipating volatility. It's really about is there a legal framework to ensure that reasonable consumer expectations for whenever or whatever that thing is that's happening in the background comes to fruition are established. Right?

So whether it's a payment system, or whether it's logging intellectual property, or recording real property, those are ways that it can be used. But I think right now what we're really looking at is these really-- I mean, here in America, as was said, this depends on where you are-- is we're really just looking at financial service providers who are truly acting in many cases as intermediaries. So it's really not about the guy in his basement with the computer mining, and then building his own wallet.

It's really about these companies that are stepping in between consumers and their value. And so that's kind of the question right now that I think is really ripe for conversation around the legal framework and governance and some other things that we've talked about. And that really comes back again to Peter's question about open or closed.

And that's why this is so complicated is what are you doing? And then what needs to flow from that? So it's really about the activities.

So I need to first-- I'm about to say something controversial. So I first need to say something I should have said at the start, which is, I'm speaking for myself. My views don't reflect that of the commission or commissioners.

To piggyback on Perianne's point, we do need a lot more education. By that I don't just mean consumers, I mean also regulators, I mean also people who are involved in these conversations, even at large financial institutions. I've noticed there is sometimes a divide between people who can discuss this in detail like everyone in this panel can, and those who are advocating for it who honestly have a fleeting understanding of what this topic is.

Which can lead to both benefits. You get more research into it. You get more investment in it. And dangerous because there's a risk of over-promising.

Now I also was going to say this. I'm glad we're focusing on intermediaries, because fundamentally, one of the big advantages and disadvantages of the blockchain is that it can reduce the role of intermediaries. Now the thing about intermediaries, especially in finance, is they are designed to increase trust. Having a third party check is meant to prevent a risk of something going wrong, often of human error.

If we take that away, that comes with some dangers. That said, if you are in the developing world where there is no infrastructure or weak rule of law, the benefits to this are tremendous, because there's really no downside. The advantage of getting around a country where the rule of law is nonexistent or is somewhat corrupt means this is just a pure win-win.

Here in the US though, if you take away the intermediary, that carries benefits of speed and efficiency, but a disadvantage [INAUDIBLE] is that if there is someone engaged in an application of the blockchain that takes advantage of consumers for whatever reason, it's harder to get the money back. Which was the point I think you made, Peter.

If I say give me a dollar, and then I want it back. No.

PETER VAN VALKENBURGH: Just kidding.

JUSTIN SLAUGHTER: That happens a lot in general on the internet for a whole host of reasons, in life too. So I do think there is a real danger of people running at this to what Kyle said. Right. I mean, we saw that with the internet too, especially all the people who were investing in irrational ideas because they told they could get rich quick.

I don't think we're here yet. I think we're lucky both from that experience and from the fact this is so complicated, it's not yet accessible to the general public. But we have to move with caution on this, because there is a danger both to the consumers-- and if people get hurt in this process too soon, it will discredit the technology to the general public, which will be a tremendous waste.

PETER VAN VALKENBURGH: So this fits in well with what I was going to say, which is you can code some things into the software client that runs on the edge of the network such that even if sovereignty exists at the edge, even if security and control exist on the edge of the network, the user interface is intuitive to the customer. And you can even potentially encode to a certain extent anti-fraud measures or consumer protective measures.

Now this sounds kind of crazy. How can you have consumer protection where there isn't an intermediary? Really, it's the intermediary designs those protections into the software. And they run locally on the user-end device.

We can understand this actually fairly easily if we think of Signal, the encrypted messaging app. There is no intermediary per se here. I mean, messages are routed. But they're encrypted on the end-user device.

Signal is acting as a privacy protector-- the developer is acting as a protector of the person's privacy-- by encoding rules that should protect their privacy onto the device. Now what does that look like in the context of payments?

An example is a multisig wallet. So we've talked a little bit about public and private keys. I'm not going to go over that again. Suffice it to say that a transaction can be broadcast to the bitcoin network that would require if anyone wants to spend in the future from that transaction two of three private keys to sign a message sending those funds on, or even 15 of 15 keys to sign a message for the transaction to go on.

Why would you do that? It's because this is the very beginning of smart contracts, really. This is programmatic money.

Now what can you do then? You provision the customer with a wallet product that safeguards one key. You allow the customer to back up a second key onto a USB thumb drive. And you say two of three keys will always be required to spend funds. And we're, the company, going to retain the third.

Now what they'll do then is use machine learning in an artificial intelligence to do the same fraud protection that credit card companies do. Is the person trying to initiate a transaction from a geographic location where their device has never been before? Is that the person trying to buy coffee in the airport? Or is that because their phone just got stolen and moved overseas?

If everything looks good, the multisig provider in this case will turn their key, along with the customer turning their key on their device, and the funds will move. If something looks suspicious, they won't. At that point, the customer needs to engage with the company, say, hey, we need to actually move this money. I am in the airport. And the funds will go.

But there's an interesting wrinkle here. What if the company goes out of business or gets hacked? Just like Target got hacked. Just like most centralized intermediaries will inevitably be hacked, because perimeter security is never enough.

Well, in that world, all you got was one key of three for all of BitGo's customers, which means you don't have any money from-- BitGo's a multisig provider. I'm just using them as an example. You don't have any money of any of those customer devices. And the customer with the multisig provider now missing goes and finds their backed up thumb drive-- it's like two factor authentication-- and signs of a transaction on their own without the intermediary.

This is a really interesting consumer-protected paradigm shift, because you can actually bake a lot into the user device from a consumer perspective standpoint. And you can eliminate a lot of weakness and vulnerability at the center of the network, which is where a lot of-- so identity theft is probably the most damaging thing in our country from a consumer perspective financial standpoint, given that we lose more money to identity theft crimes than all other property crimes combined. Billions of dollars every year.

And this is a technology that can actually potentially make real inroads to that problem, because if you don't have a centralized intermediary like a credit card company or a Target that's holding a bunch of personally identifiable information, which can then be used to make fraudulent transactions on their behalf, if you don't have that weak point in the center of the network, that problem starts to go away.

AARON WRIGHT: But you're likely going to have intermediaries. We've already seen intermediaries emerge in this space. Peter mentioned them. Coinbase.

Again, there's been analogies to this technology-- the internet. I don't think they're exactly on point. But there's some things that are parallel.

One way think about this, especially if this is an area that you study, this is kind of another application layer of the internet, much like HTTP. It's kind of sits in between the TCPI layer in the internet stack and the application layer. So it kind of almost forks it a little bit.

And on top of that application layer, people will use blockchains. And they'll be intermediaries. They'll be like Coinbase. They'll interact with that application layer, this blockchain-based protocol.

Or they may just be open source software. Right? And the user interface may emerge to a user in the form of open source software. And that raises significant and challenging questions. It's really hard to stop open source software that's widely demanded once it's released to the public.

The last thing is that it's beginning to get embedded into browsers. So there's already plug-ins where you can plug-in into Chrome, I think Firefox, a simple Chrome plug-in. You can set up a wallet, load it up with some virtual currency, like bitcoin or other virtual currencies. And then you're off to the races. You can interact with these applications.

BlockEx another example. So I think you're going to see, much like with the internet, it's going to manifest in a number of different ways. But I think, as Peter described, it's super hard to follow a lot of times, securing bitcoin. This is really early days. This is like early websites where everything was blinking, things were all turned around. So we have a long way to go.

But I think the ecosystem will develop in such a way that there's intermediaries. There's also interaction just directly through a browser. But the most interesting, especially for consumer protection concerns, is what happens when it's open source? What happens when there is no intermediary that's really involved? And how do regulators deal with that at that point?

When it's an intermediary, I just mentioned, it's not that different of an analysis. When you have open source software that's interfacing with autonomous smart contract programs, and they're doing things like building marketplaces to buy and sell things that are called tokens, of which $100 million have already been raised to them.

What does that mean for the securities industry or securities laws? When you're building a prediction market where you can begin to bet on future events, something that the CFTC has looked at. And that's actually just open source technology, well, what's the CFTC to do at that point? If consumers are saying they want it, who are you going to turn to at that point to clamp down?

JUSTIN SLAUGHTER: How do you censor it? And in fact, one of those things wasn't following our rules. So they did get shut down, actually. [INAUDIBLE].

I actually think this is a really good point, because I'm reminded, in fact, on securities. There is a concept that may be used for this for open source. In securities law, or certain kinds of small offerings, we deem that the protections for the users can be less if they are quote/unquote "sophisticated investors."

And that basically, I sign up. I understand the risk. I affirmatively waive my right as a usual securities investor We give you access to additional gardens of opportunities. But the flip side-- something goes wrong there, you're more on the hook. There's less we can do.

That might be the kind of mindset we have to use for a purely open source where it's a-- trying to think of the Latin for it-- basically enter at your own peril.

AARON WRIGHT: Caveat emptor.

JUSTIN SLAUGHTER: Caveat emptor. [INAUDIBLE]. But without question, that has to be the mindset that we understand the risks attendant to this, and ensure that there are checks in place before people can just sign up. That could be as little as checking a box. We can debate whether that's efficient at all, because too often it seems people are willing to just run right in and throw caution to the wind.

The vignette I've used in the past is whenever you get a cell phone contract, it's huge amounts in terms in there. I've never seen a person read all the way through.

My contracts professor in law school, 15 years ago, in fact, told me he tried to read through it once. It was two days. It didn't make any sense to him.

So we have to be aware of how the system we're using works. I don't know if there's a technological solution for that. Maybe there is in terms of requiring people to have a basic knowledge of cryptography of the blockchain. That could be very limiting to users, though. But that's one option.

KYLE BURGESS: Something that came up-- I don't know how much of the audience is overlap from earlier. But in the AI panel, they talked about the government not hiring enough people with the appropriate technological experience. That might have just come up earlier, too.

I think as a consumer of the internet, I trust that my emails are encrypted when it says that it's encrypted. I have no idea what that means. I don't understand what a TCP protocol is or does.

I think there's only one coder on the stage, maybe 1 and 1/2, who actually gets some baseline understanding of what the technology and how it works and what it does in terms of the actual coding piece. So I just have to take everyone who is smarter than me at their word when they say that this is what it is, and this is how it works.

PERIANNE BORING: Not smarter. Have skills in different areas. [LAUGHTER]

KYLE BURGESS: I'm going to go ahead and say Peter's probably a little smarter.

PETER VAN VALKENBURGH: No, no, no, no. I do not-- I am not a cryptography expert, and would very much rely on other people for that work as well. It's always a matter of trust.

KYLE BURGESS: Yeah. And you know, I think for this to have value for consumers, we need to get to the point where just like when I send an email, I can trust that that's encrypted because it's kind of been proven, I think, for this to direct consumer use of this, we do need to be at a place where consumers actually can trust that it is what people purport it to be.

PETER VAN VALKENBURGH: Open source-- Oh, sorry.

KYLE BURGESS: No. Sorry And what companies-- we've already seen in the last three years a number of companies come and go, because what I think Perianne mentioned earlier, there is all these grand ideas of how it can be used. And those companies have come and gone, because blockchain is not the solution to everything. And there are other solutions that can solve these problems. People aren't calling them blockchain problems.

But until we get to the point where I think you can just-- it's kind of been proven, I am wary to say consumers should just go for it.

PETER VAN VALKENBURGH: I was just going to say that I think we've talked a little bit about open source. Open source is part of the answer here is that especially the permission list networks. But even the permission networks now are all being developed in an open source manner under the presumption that with enough eyes on the code, all bugs are shallow. Linus's Law.

But to be totally forthright, I mean, there've been bugs in the Linux kernel that have just sat there and persisted for years undiscovered-- at least undiscovered publicly, and maybe privately discovered and exploited. So this is an intractable problem, though, I think. As our world becomes technologically more advanced, whether because of blockchain or because of artificial intelligence, the spaghetti code that underlies so much of it becomes quite the liability.

But I think we'll go on and just hope that it's all going to be fine.

KYLE BURGESS: A lot of the issues that have come up so far with that digital currencies and blockchain technologies aren't even related to the technology. People are just bad actors, sometimes. And so a lot of the scandals that we've seen come out about this have had to do with bad actors and not having good protocols, not on the protocol, but just good protocol in place for being good fiduciaries and taking care of consumer protection issues.

ELIZABETH KWOK: Yeah. And I think that you all have kind of been going around this general issue that the FTC is interested in, which is in these early days where you're kind of bouncing back between open versus where there are intermediaries, a lot of issues that are very common, such as data security, from a consumer perspective are very bewildering, because how do you participate, but do so in a responsible way? And as Kyle just said, there are going to be malicious actors who take advantage of this environment.

So I'd be curious to hear perhaps from Christina from a consumer perspective in this world-- this new wild west-- with respect to data security, and as Peter pointed out, it's being pushed out to

the edge in a lot of these systems, how should consumers be looking at this? And what should they be on the lookout for?

CHRISTINA TETREAULT: Sure. I would say that the short answer is a yellow caution light. And a good disclosure is never going to save a bad product. So I'm a little leery of the consumer education piece.

We're really eager to see providers bake in the consumer protections. Technologies going to outrun consumer protection under law, unfortunately. But that doesn't mean that providers can't act ethically and do what they can to ensure that these are safe products. You don't want the equivalent of an exploding toaster behind the scenes.

And I think the other piece of this though is understand that generally speaking with these technologies, whether you're using them for financial services or otherwise, in the absence of a legal framework, there is really no one to call when something goes wrong. Right? So understanding that you probably will have to have a very lengthy court case using some sort of established law in order to get some sort of resolution for a problem you encounter, it's something that folks should really maybe pump the brakes in terms of thinking about whether they want to jump in.

In terms of optimism-- because I'm fundamentally an optimistic person, so I want to frame this also though-- is that you've heard on this panel all these amazing applications for this. And there are incredible people working very hard to figure out how this can work so your refrigerator can order you eggs. And it doesn't end up being a catastrophe.

So I'm optimistic in terms of having these solutions solved. But I would say that there's still that yellow caution light for folks who are interested in jumping in.

PERIANNE BORING: We're also seeing an evolution of the legal and the audit industries, because so much of this is technical. This is something that we've spent quite a bit of time discussing in our smart contracts alliance is an initiative of the chamber that includes academics, legal professionals, accounting professionals, and also technology professionals, to companies that are billing smart contracts capabilities. Smart contracts will play a big role in the adoption of blockchain technology overall.

And what we're seeing is that while so much of agreements are turning into code, there's going to be an evolution of legal to audit. So if the code is also part of a contract, or is referenced in a contract, does the lawyer also have to be a coder? How do you audit the code?

And we think we're going to see a big evolution in-- and also a coming together of the legal and the audit industries that the lawyers will also have to have a coding background. And the auditors will also have to work more closely with lawyers, because the legal and the code is beginning to come together.

AARON WRIGHT: I think the key thing with security and blockchains is that blockchains rely beyond the peer-to-peer network a consensus mechanism and the actual data structure on public private key cryptography. So everybody gets a public address that's like an email address. But every email address, in order to actually send an email, you need a password. That's the private key in the land of blockchain technology.

But unlike email providers or other services that may actually enable you to remember your password to regain access so that you can send emails, when you push it to the edge, that private key, which is your access to these blockchain-based networks, becomes incredibly important. And there hasn't been great solutions or fully comprehensive solutions on about how to manage that private key.

So imagine in the future-- we push 20, 30, 40 years in the future-- we're actually using these systems for important things like our personal wealth to hold our stock accounts or other assets that we may have. And that gets stolen from us through a cyber attack. Our computer gets infected. That gets stolen. Maybe it's now ransomed us in some sort of way.

There's nobody to turn to to get back that password. There's nobody to ask to say, hey, can you remind me what that password was? Because right now those passwords usually have to be quite long. Where they're suggesting that they're quite long in order to maintain security. So that aspect is exceptionally cumbersome. It's rife with consumer protection problems.

I think the second area that's incredibly important is privacy. So Peter mentioned this. But bitcoin, it's not anonymous. It's pseudonymous. And as researchers have shown-- and it's pseudonymous because it actually leaks metadata that various transactions. So as research has shown, you can take that metadata and analyze it through something called transaction graph analysis, and actually begin to de-anonymize people on the network.

So we're actually building what could arguably be another layer of the surveillance, another layer where not only are communications being surveilled, but also transactions can be surveilled. And because nobody sits in the middle of that, and if this gets widespread adoption, that raises significant concerns.

Well, I'm not concerned that that would happen in the US. I am fairly concerned that that would happen in other countries that are much more repressive, like China or Russia or other countries along those lines. And these are not new risks. People have talked about the issues related to e-cash, digital currency for years.

But just to kind of put a point on that, back in the '70s, there actually was a group of academics that were convened with one question-- how can we build the most insidious surveillance technology? And they assumed that this would come from Russia. Or the USSR, at that point.

Their answer-- it was not the internet. It actually was a traceable digital cache. And that's been built. And that is fundamentally what bitcoin is.

So there's a number of privacy-related questions that are emerging with blockchain technology, with bitcoin. There are solutions-- like ZCash is a potential solution. But we can't forget about that as we begin to see the widespread adoption of these technologies.

COLIN HECTOR: And to sort of piggyback on that, so panelists have sort of identified some of the security and privacy issues that are raised by this technology. One of the big remaining questions that I'd like the panelists to comment on is, how do we approach this from a regulatory standpoint? Is this something-- and that might be nuanced. Maybe there's not a one-size-fits-all here.

Things that got raised in the last panel include the regulatory sandbox, is there traditional modes of regulation, with the prepaid card rule, or Red E, or even things like state licensing. And I'd like to start with Justin.

JUSTIN SLAUGHTER: I think probably the first step is to be some kind of a sandbox. The question is going to be what that entails. Everybody can say build a sandbox. But the details matter a lot.

Are we trying to encourage innovation such that we limit it to certain kinds of startups? Are we trying to let everybody have it? These are the questions we're going to have to work with.

I also tend to think, personally, because there is no clear regulator, we should probably I would say immediately consider forming some kind of interagency task force to deal with all these jurisdictional questions.

PERIANNE BORING: But is that another layer of bureaucracy?

JUSTIN SLAUGHTER: That's the problem. These are the choices we get to make. I would probably call it more of a consulting group. I would also say the additional problem is it adds more time to this, because then that can run on for months, or you're even moving quickly.

PERIANNE BORING: What do you mean a consulting group?

JUSTIN SLAUGHTER: I mean, you literally get a bunch of the various regulators together to talk about this and figure out as a starting point who has jurisdiction over what? Because we have had times on other issues where one regulator will literally enter a court case by where a private person is suing over say, a government action, say, we're siding with the private entity. We think the government's wrong here on jurisdiction.

That carries real risk then, because then you're in a legal battle. And that can drag on even further.

PETER VAN VALKENBURGH: An interesting issue on that that amplifies the problem here in the US is that so much of the regulation is actually done at the state level for consumer protection purposes because of a very convoluted history of money transmission licensing law that led to companies like PayPal and Venmo being classified as money transmitters rather than as chartered banks.

And then the assumption when digital currencies come around, that companies that hold other people's bitcoin for them would be like a Venmo or a PayPal, and therefore should also go down the money transmission route. That's a very interesting approach. I think it's generally a poor approach for the US as compared to more unified jurisdictions like the UK with the FCA, or Singapore's monetary authority who have taken a more holistic we'll look at the whole thing and you'll have one point of contact with a regulator to help you understand your obligations to make sure you're compliant on all these things.

And at the state level, you'll find all sorts of varying levels of sophistication with regard to the technology. Some will be very eager as regulators to get involved and to make sure consumers are safe-- maybe too eager sometimes because they'll move too quickly. And others will basically not answer your calls if you're a business that wants to be regulated and wants to be consumer-protectant. But they don't know what you're doing and aren't interested in giving you a license to operate in their state.

Additionally, just the patchwork regulation we have for money transmission is probably worth questioning, even in the PayPal context where people might hold large and substantial balances in their PayPal account. It's kind of interesting that those balances aren't FDIC-insured. You're an unsecured creditor of PayPal.

And they're being regulated at the state-by-state level. So in Alabama all they had to do to comply was to post a $10,000 bond for the benefit of customers in Alabama. I'm pretty sure there's more than $10,000 that they're holding for people in Alabama.

JUSTIN SLAUGHTER: I mean, this is where it's ironic, right? We want to encourage the innovation of a decentralized network. And it is in some ways being impeded by the fact that our system of regulation is itself decentralized.

We have seven notable financial regulators, all of which would have the same [INAUDIBLE], not to mention consumer regulation like FTC, like-- we have 50 state regulators, basically. This is the kind of thing you would say, well, normally the solution is you have legislation. I think asking for Congress to legislate on this would be a mistake.

PERIANNE BORING: It's probably not going to happen.

JUSTIN SLAUGHTER: I think it's not going to happen. I think it probably would only do more harm than good, which is we have to work with the system we have, which that's the problem then, because the first step is figuring out who should be the person who is the primary.

PERIANNE BORING: And again, we don't want to pass laws and regulations in a nascent period of the technology when it's still developing. What I think we should do is have best practices. We've certainly looked at doing this many, many times.

And best practices, if anyone has participated in creating best practices, it's a very expensive process. It can take years to finalize them. I've met with a lot of trade associations that represent more mature industries, and literally millions of dollars the industry has had to pay to get these best practices out.

But they've been incredibly effective, especially with the FTC. And at least having something that the industry can point to as, this is what's fair. These are some guidelines to go by.

But again, it's expensive to do that. And a lot of the companies that would really benefit from this-- they're small companies. They're private companies. They've raised maybe $100,000, maybe $60 million. But they don't have millions of dollars to throw at best practices. They're building technology. This is finding a line item in their budget for that is hard to do.

So perhaps that's something the industry and the FTC can do.

KYLE BURGESS: For the best practices, it is expensive. But one solution that we've worked on is crowdsourcing it. So I mentioned earlier, we do a conference in Bretton Woods. This past summer we did consumer protection with digital currency and other assets, digital assets. And we used some of the bright brains on this stage, Peter being one of them.

We've worked with getting commentary from FTC, commentary private, because they can't endorse any product of ours. But just kind of feedback from the different agencies until they get set up. So like with the peer-to-peer lending industry, what they did was they set up a list of like consumer bill of rights, and then guiding principles to make sure that those bill of rights were protected. And then they were ultimately regulated while regulators figured out what they wanted to do with Lending Club and Prosper.

And it is state-by-state regulation. So we're hoping to do a similar thing with bitcoin and blockchain is work with the different key stakeholders now, both in government and also the businesses, to develop guiding principles for those businesses, and then get the companies to adopt them, or at least as a starting framework.

Best practices gets difficult because each different business has its own business model. And you don't want to get into the business model of how that's run. So like where we ran into trouble was usability, like the UX, UI stuff for the interface of the technology. I think Christina mentioned it earlier. Baking in a lot of consumer protections into whatever it is that the consumer is engaging with will solve a lot of the problems.

But when we started to say, dive down that rabbit hole of what different things needed to be in place, it got really complicated, because the money transmitters had different things than the exchanges have than the wallets have than the whatever.

And so we decided on a 14 right list of consumer rights. And then a accompanying guiding principles. And we've been talking with different blockchain-based businesses about adopting it. And we're still taking feedback on the document. So if you want to give feedback, see me afterward.

But yeah. I think right now we are-- while the government figures out its task force or the consulting thing, while we're in that kind of nebulous unclear area, there is an opportunity for self-regulation until that problem is solved by--

JUSTIN SLAUGHTER: I mean, look. I actually think in general, where the industry best practices are strong and rigorous and do the job, regulators like to sign off on that. We've done that in tech recently with cybersecurity protections. We're working on a number of other issues related to nascent technology.

If the industry can come together on that kind of not a minimal level, but a fair level of protection for consumers, and bake that into either the tech or to a bill of rights, that goes a long way.

AARON WRIGHT: Yeah. But self-regulatory organizations oftentimes become racist to the bottom. So that's concerning. I think one key thing that just needs to be kept in mind is that blockchain technology is not simply a financial technology. It's going to hit a number of different-- to use a term used in the past panel-- silos. We've already discussed a little bit how it's going to hit when it comes to payment systems, money transmission, and [INAUDIBLE] know your customer laws.

When we talk about smart contracts as legal contracts, we're talking about how it interfaces with the existing common law contract system that we have. When we're talking about how you can tokenize trade securities, we're talking about securities laws. And not just securities laws, but other very complex regulatory regimes like Dodd-Frank. What happens if we have peer-to-peer exchanging of securities? Are we getting rid of clearing houses? Will that lead to significant financial instability?

We have questions related to privacy law. What's going to happen here if you begin to build these systems that are leaking data in certain ways? We also have questions of when we begin to build virtual corporations about corporate governance. How are these organizations is going to be administered?

And then when you begin to think about machines, it blends into the whole AI discussion about ports and other things like that. So I think as we've learned from the internet, sometimes doing too much a priori thinking-- or too much a prior regulation-- just doesn't work. We're not great at predicting the future. We don't know where things are going to pop.

Nobody could have contemplated in 1996 that Facebook would have billions of users across the globe, there would be this whole social media revolution, or very few people could have. And I think we're in a similar spot.

We know that this has got a lot of potential. We know that there's a lot of interest. But we don't know where it's going to go.

So one idea-- and something that the US did do under the Clinton administration-- is the nation actually developed some guiding principles themselves, which may help here. Do we want to have what we seem to have adopted with the internet, an end-to-end principle with this? Do we want to place more regulations at the middle?

We chose not to when it came to the internet. And there's costs related to that-- costs that we're still trying to sort out. I think a serious conversation needs to be had in order to distill those principles. I think it's great what's happening in terms of best practices. Maybe that can feed into that.

But I do think that government has a role here to actually shape and mold the development of this technology. But we need to think about it not just as a financial technology, but as a broader based technology.

CHRISTINA TETREAULT: And I would just second that activities-based regulation is appropriate. And that industry self-regulation has not proven most protective for consumers. And so that's worrying.

And then the last piece of it being that a lot of these technologies were sold in early days around increasing financial inclusion. And the last people we want to be seeing-- the last set of consumers that should be targeted for practice runs are people who are already not included in the larger system. So you know, it's really about having sensible safeguards in place, rules of the road, so that folks can have a clear understanding of what they can do if something goes wrong and figure out how to solve it. So.

PETER VAN VALKENBURGH: I'm actually optimistic also for that kind of regulation from government to address what Justin wisely called the decentralization problem of US financial regulation in this case. There are some promising signals. So the OCC's FinTech Charter Initiative is one thing to look at, where the OCC, which is a branch within Treasury, is now contemplating basically chartering FinTech companies as special purpose national banks, as long as they engage in one of the three core activities of banking, whether it's deposit taking, lending, or access to the payment system.

And all of these virtual currency companies that are currently going the 50-state licensing route and holding other people's bitcoin for them, in need of consumer protection, I would say, would potentially be classified as doing that access to the payments system function, and would be potentially eligible for a national special purpose charter.

This is almost sci fi, because the OCC by their own admission has never been the most bold and innovative regulator out there. But they seem open now. And that's very encouraging, because it could be a way to lower the cost of innovation from going the 50-state route, while still making sure that there is a single regulator really looking out for the solvency of the organization and the protection of their customers.

The other thing I would stress is that these money transmission laws are drafted so broadly that they could apply to people who are doing little more than merely developing software, that is infrastructure on these networks that actually powers the ability to push control out to the edge, and often powers the ability to do the sort of consumer protection multi-signature applications that I was describing earlier. We don't want to be imposing costs on those businesses unless they really are holding other people's funds.

So rather than trying to go state by state and clear up the definition of money transmission to make sure that those companies aren't required to get a license for writing software, I'm actually somewhat optimistic maybe about representative democracy at the federal level that we could get a federal safe harbor for non-custodial development of the technology, noncustodial software development, infrastructure development. Because that's where you want as much iteration as possible so that the user interfaces, which are all software, get better so that the customer is better educated by the app that they're using themselves to actually be protected.

And those are also instances where the developer isn't actually capable of ever running away with the funds, because they never had custody of them to begin with. They're building pipes, not reservoirs.

AARON WRIGHT: And that that would go along the lines of what we adopted with the internet. An end-to-end principle.

PETER VAN VALKENBURGH: Exactly.

AARON WRIGHT: We're going to clear out the middle. We're going to allow a lot of innovation. We're going to place regulation around the end point.

I do think that there's also a risk or just overregulating too soon. Right. So this happened actually back in England with cars. There used to be something known as the Red Flag laws. So everybody saw a car. And they knew that it was dangerous, right?

So England promptly regulated it. And they passed a series of laws, some of which actually got adopted in US states as well, where they actually required three people to operate a car-- one person to drive it, one person to fuel it, and one person literally to stand 30 feet, or some number of feet in front of it, waving a red flag to tell people that it's dangerous.

Now it's sensible, right. We knew that cars were going to be dangerous. We knew that they could hurt people. But even though England was one of the forerunners of the automotive industry, it didn't really take root in England the same way it took root in Michigan, where they didn't pass a law like that. So I think there's always a risk of overregulation.

I think the risk is particularly pronounced here, going back to the actual characteristics of a blockchain. So because it's disintermediated, because you can build autonomous software, and because its transnational, people just may not care. They may just release the software.

And they actually may be that Nietzsche who's driving that car. They have a specific perspective. They want to push it. They're going to release it. And if there's demand, it's going to be really hard for it to shut down.

And to a certain degree, you can view bitcoin like that. You know, bitcoin has embedded into it very particular biases. Right?

The first block of the bitcoin blockchain has an expressly political message. It was released on the eve of the Second Bank [INAUDIBLE] in England. It has embedded in it a fixed currency, which appeals to a number of people who think that we should go back to a gold standard. So a lot of its early adopters are people who believe in that.

And whether or not that's a good or a bad thing, that's not really-- I don't think we need to get into it. But just know that these are all really hard to shut down systems that are autonomous that are going to have certain values embedded in them. And if you regulate too quickly, and certain people get upset with that, they're just going to release them into the wild. And we're going to have to grapple with that if there's a lot of demand for that. So those are the risks kind of at play.

COLIN HECTOR: And although we have a lot more that we could talk about, clearly, we are running up against our time limit. So I want to thank all of our panelists for participating today.

And I'm going to turn it over in a second to Duane Pozza to give some brief closing remarks. [APPLAUSE]